

# DATA SECURITY



## Artificial Intelligence: Data Security and Privacy Tips

When instructors incorporate AI tools such as chatbots and generative models in their teaching, they must focus on safeguarding data privacy and guiding students on ethical usage. Here are key points for instructors to keep in mind:

- **Review Data Collection Policies**

- Carefully review the data collection and usage policies of any AI tools you implement. Understand what information is gathered and how it is stored.

- **Anonymize Student Data**

- Avoid directly uploading students' personally identifiable information into AI systems. Anonymize or pseudonymize any student data used as much as possible.

- **Data Collection**

- Configure AI tools settings to minimize data collection from students where options exist. Disable storage of user conversations and usage logs if they are not essential for educational purposes.

- **Educate Students on Responsible Usage**

- Have open conversations with students about behaving ethically when using AI tools as students and instructors.

- **Allow Students to Opt Out**

- Provide students options to limit data sharing with tools if they have privacy concerns. Also, allow them to opt out of using AI tools entirely without penalty.

- **Get Consultation When Unsure**

- If any uncertainty exists around privacy protections or appropriate use of specific AI technology in the classroom, seek guidance from your supervisor before proceeding.

While still an emerging issue, taking deliberate steps around user awareness, secure configurations, limited data sharing, and purposeful data minimization allows instructors to explore the beneficial uses of AI responsibly. Continually reevaluating privacy risks against educational value is critical for adoption.

## Protecting Data Collection in Common AI Tools

### OPENAI'S CHATGPT

#### New Ways to Manage Your Data in ChatGPT

OpenAI introduces a feature allowing users to disable chat history in ChatGPT, ensuring previous conversations aren't saved or used for AI training. Although new chats are stored for 30 days for abuse monitoring before deletion, existing conversations with history "on" may still contribute to model training.

Users can adjust settings in their ChatGPT account to toggle off chat history and export their data, with an option to swiftly re-enable chat history if needed. OpenAI gives step-by-step directions and a visual demonstration of how to do this. Use the article link to read and learn more.

- [Manage Your Data in ChatGPT](#)

## **GOOGLE GEMINI**

### **How to Stop Gemini From Storing Your Data and Location**

Gemini's Privacy Hub page provides a discussion concerning the company's data collection, human review, data management, and legal summaries. The company also provides clear guidance on how individual users outside of schools and workplace accounts can manage and delete activity in the Gemini Apps. Users should note that when Gemini Apps Activity is off, your conversations will be saved with your account for up to 72 hours to allow Google to provide the service and process any feedback. If you'd like to adjust the auto-delete settings for your Gemini Apps activity, you can do so by following these steps on Google's information help page.

- [Gemini App Activity Management Instructions](#)
- [Gemini Apps Privacy Hub](#)

## **CLAUDE**

### **How Does Claude AI Ensure Data Privacy and Security?**

Claude does not have a data toggle on or off switch; rather, the company's platform rests on how its AI prioritizes data privacy and security by implementing strict measures. Claude minimizes data collection, encrypts stored data, undergoes external audits, and upholds responsible AI practices. It does "not use Inputs or Outputs to train their models." Additionally, the platform offers user control for data deletion. It promises not to sell or share user data with third parties, aiming to set new AI privacy and security standards. Users are encouraged to read the company's Consumer Privacy Policy.

- [Claude's Privacy Policy](#)
- [Navigating Privacy Concerns with Claude AI \(2024\)](#)

## **MICROSOFT COPILOT**

### **OSU offers Microsoft Copilot with commercial data protection to faculty and staff.**

We recommend using Copilot for AI chat to help keep our institutional data safe with built-in commercial data protection from Microsoft. To receive full data protection, you must sign into the Copilot using your institutional username and password. Learn more about OSU's Copilot AI by watching the video below and reading "Getting Started with Copilot."

#### [Overview Video of Microsoft Copilot](#)

#### [Getting Started with Microsoft Copilot](#)

# Other Resources

---

## Campus Resources

- [OSU Information and Technology Department](#)

## ITLE Resources

- [Instructor Guide to Chat GPT & Other Generative AI Software](#)
- [Student AI Guidance](#)

### **Generative Artificial Intelligence Chatbot Usage Policy**

This document provides General Guidelines for adopting AI in the workplace. Click on the title to access the full document.